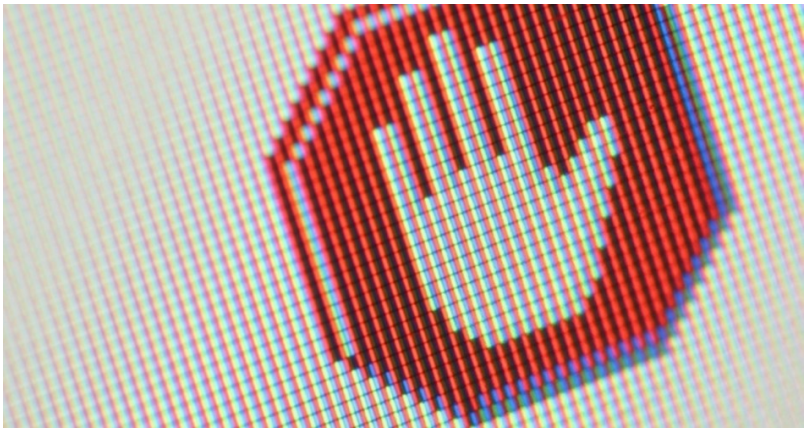
Written by **C. Mitchell Shaw** on March 22, 2016

FBI, DOJ Postpone Hearing in San Bernardino iPhone Case



The FBI and Apple will not get their day in court. At least not yet. The hearing over whether Apple must weaken the safeguards around its own encryption at the behest of the government — scheduled for Tuesday — was postponed by the Justice Department at the last minute. The FBI is now saying what tech experts have been saying all along: There may be a way to get into the iPhone used by the San Bernardino shooter without forcing Apple to create a backdoor.

Politico reported Monday:

> Citing a new possible way to access a locked iPhone used by a shooter in the San Bernardino terrorist attack, the Justice Department on Monday convinced a federal court to cancel a Tuesday hearing on whether Apple should be forced to help the FBI break into the device.
>
> Government lawyers had insisted for months they needed Apple to write special software so the FBI could bypass security features on the iPhone being used by the San Bernardino shooter, Syed Farook, and obtain what could be critical information for their ongoing terrorism investigation.

The FBI may claim that there is some "new" way to do this, but as *The New American* reported last week, this way is not new at all. When the FBI claimed, "Apple has the exclusive technical means" to access the data on the iPhone 5c used by Syed Farook, NSA data-analyst-turned-whistleblower Edward Snowden responded by saying, "Respectfully, that's bullsh*t." He added, "There are hardware attacks that have existed since the '90s that the FBI can mount" that would give them access to the data on the phone. The ACLU even published an online article that spells out — in detail — one way in which the FBI could gain that data without forcing Apple to create a backdoor into the iOS platform. As this writer said then:

> When the phone — which is actually owned by the county of San Bernardino and was issued to Farook as his work phone — was recovered by San Bernardino investigators, they were instructed by the FBI to change the password of the iCloud account associated with the phone. This prevented the phone from being able to backup its data to the iCloud service where it would have been accessible to the FBI since Apple does hold the keys to the encryption of that service. In fact, Apple has made all of the data from the iCloud account associated with that phone available to the FBI. But, as the FBI claimed in its petition to the court, changing the password made the data "permanently inaccessible" since Apple does not hold the encryption keys to iPhone and iPad devices.
>
> If the FBI had not directed San Bernardino investigators to reset that password, there is a good chance that simply by connecting the phone to one of its default Wi-Fi networks, it would have sent much, if not all, of its data to the iCloud where Apple would have been able to access it and turn it over to the FBI. In describing the decision to reset the iCloud password during his testimony before Congress, FBI Director James Comey said, "There was a mistake made." It is unimaginable that a

> computer forensics investigator working for the FBI would make such a "mistake."

It is apparent that the FBI's motives have little to do with the data on this particular device and much to do with setting a precedent in regard to all encrypted devices. From that same article:

> The iPhone at the center of the FBI's PR and legal war against Apple was not even Farook's primary mobile phone. He had a personal phone which he destroyed before he and his wife went on their ISIS-inspired killing spree. Let that sink in. Farook had two phones: a work phone and a personal phone. His employer has access to the itemized bill on his work phone which would show every number he called and every number that called him. In fact, Verizon has given the FBI a record of all his calls and texts. He did not destroy that phone, but he did destroy his personal phone. It doesn't take The Amazing Kreskin to figure out which of those phones he was worried about investigators accessing. It is highly unlikely that anything of any value to this investigation could be found on the phone the FBI is making such a fuss over. So, why all the fuss?
>
> If the FBI can access the data through well-established methods and there is little likelihood that the information it claims to seek is on the phone in the first place, why would the FBI scuttle the easiest method and then ignore the most effective method at its disposal? The simplest answer is that the FBI is not interested in Farook's iPhone; it is interested in setting a precedent in regard to all encryption.

Now, the FBI is telling the court that — voilà — it has found a way to do what it said could not be done. In a filing with the court, federal prosecutors said, "On Sunday, March 20, 2016, an outside party demonstrated to the FBI a possible method for unlocking Farook's iPhone. Testing is required to determine whether it is a viable method that will not compromise data on Farook's iPhone. If the method is viable, it should eliminate the need for the assistance from Apple Inc. ('Apple') set forth in the All Writs Act Order in this case."

Of course, there was no mention of who that "outside party" is or what "possible method" was demonstrated. Perhaps someone in the FBI finally got around to reading up on the subject. More likely, the FBI realized that the likelihood of winning its case against Apple had already greatly diminished when a federal judge ruled against the agency in a separate, but related, case and that as news of the ridiculousness of its claims was coming to light that likelihood was approaching zero.

Whatever the FBI's reasons (either supposed or actual), the case is now on hold. The FBI will have to either crack the phone itself, admit that there is probably nothing of value on the phone in the first place, or crank the whole machine up all over again and go after Apple a second time. Considering that Apple's engineers have the option of resisting the order themselves, the FBI may not have much choice in this matter anyway.